

Attorney General's Office
State of New Hampshire

FAX: (603) 223-6202

Business: Advent Software, Inc., 600 Townsend Street, San Francisco CA 94103

Nature of incident: A secured and locked laptop was stolen from Advent's San Francisco headquarters office at night. The laptop was removed by forcibly breaking the lock mechanism. The laptop had boot level password protection installed in addition to the operating system username/password. The laptop contained a file with names, social security numbers, and home addresses of certain current and former employees.

Date of discovery = November 20, 2006

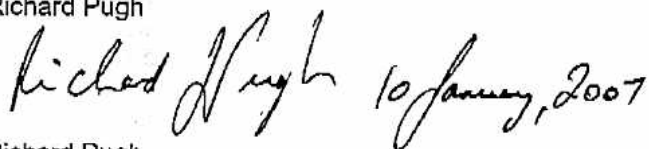
Estimated number of affected individuals in New Hampshire = 21

Date of notification, after investigation, to affected individuals

- (i) November 28, 2006 internal email from IT Security
- (ii) December 4, 2006 internal email from HR Department
- (iii) December 8, 2006 US Mail letter to former employees
- (iv) December 28, 2006 followup US Mail letter to current employees

Sample of US Mail letter is attached that describes the incident and the actions taken by Advent in response.

Regards,
Richard Pugh



Richard Pugh
Director, Systems Security & Compliance
Advent Software, Inc.
600 Townsend Street
San Francisco CA 94103
415.645.1025

Advent Software, Inc.



December 28, 2006

Richard Pugh
[REDACTED]
[REDACTED]

Dear Richard,

We want to follow up on the email notification that was sent to Advent employees on December 4, 2006 and inform you again in this letter of a recent incident that may affect some current Advent Employees, including you.

A theft/burglary occurred at our Headquarters, and we had a laptop stolen that contained a file with your social security number and home address. While we cannot be sure that data theft was the intent, we recommend that you take measures to monitor and protect your credit so you can be alerted if your information is misused.

We apologize for any inconvenience or concern this situation may cause you. Along with taking steps to improve our facilities and data security, we want to assist with reducing the impact on you, by helping you monitor your credit and financial transactions to reduce the risk of fraud.

Credit Monitoring Assistance

To assist you with monitoring your credit files, we have partnered with Experian to provide you with a full year of credit monitoring, paid for by Advent. The credit monitoring product we have selected is Triple Advantage Premium. This program will identify, and notify you of any key changes in your credit history that may be a sign of Identity Theft.

Your membership includes:

- o One 3-Bureau Report when you sign up (Experian, TransUnion, Equifax)
- o Unlimited access to your Experian Credit Report and Credit Score
- o Monitoring of all three of your national Credit Reports every day
- o Email or SMS Text alerts when key changes are identified
- o Access to Fraud Resolution Representatives
- o \$50,000 Identity Theft insurance provided by Virginia Surety Company, Inc. (Unfortunately, due to New York state law restrictions, coverage cannot be offered to residents of New York)

You have until February 28th, 2007 to activate this membership, which will continue for 12 full months following activation. We encourage you to activate your credit monitoring membership quickly. To activate your Triple Advantage membership, please visit <http://partner.experiantdirect.com/premium/> and click "Sign Up Now." Have your personal access code ready. You will be instructed on how to initiate your online membership.

Your personal credit monitoring access code is [REDACTED]. Please do not share this access code with others.

*Sample letter
for employees (4 pages)
Minor redactions of
confidential code and
home address.
Richard Pugh
Director of Systems
Security &
Compliance
12/28/06*

Advent Software, Inc.

Other Steps to Take to Protect Your Identity



We urge you to **place an initial fraud alert on your credit file**. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You may call any one of the three major credit reporting companies. As soon as one credit reporting company confirms your fraud alert, the other credit agencies are notified to place a similar alert. An initial fraud alert stays on your credit report for 90 days and is available without charge.

You have the right to ask that nationwide consumer credit reporting companies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide consumer credit reporting companies.

<https://www.annualcreditreport.com/cra/helpfaq#fraudalert>

Equifax: 1-800-525-6285; www.equifax.com

https://www.econsumer.equifax.com/consumer/sitepage.ehtml?forward=cs_cpo_howto#seven

Experian: 1-888-397-3742; www.experian.com/fraud

TransUnion: 1-800-680-7289; www.transunion.com

There are two types of fraud alerts: an **initial alert**, and an **extended alert**.

- **An initial alert stays on your credit report for at least 90 days.** You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial alert is appropriate if your wallet has been stolen or if You have been taken in by a "phishing" scam. When you place an initial fraud alert on your credit report, you are entitled to one free credit report from each of the three nationwide consumer reporting companies.
- **An extended alert stays on your credit report for seven years.** You can have an extended alert placed on your credit report if you have been a victim of identity theft and you provide the consumer reporting company with an Identity Theft Report. The form can be found at:
<http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html#Whatisanidentitytheftreport#Whatisanidentitytheftreport> When you place an extended alert on your credit report, You are entitled to two free credit reports within twelve months from each of the three nationwide consumer reporting companies. In addition, the consumer reporting companies will remove your name from marketing lists for pre-screened credit offers for five years unless you ask them to put your name back on the list before then.

How do I report fraudulent misuse of personal data?

These two web sites outline measures you can take if you believe your personal data or identity has been improperly used:

Advent Software, Inc.



<http://www.ftc.gov/bcp/edu/microsites/idtheft/>
<http://www.ssa.gov/pubs/idtheft.htm>

Here are some highlights from these advisory sites:

Once you get your credit reports, review them carefully. Look for inquiries from companies you have not contacted, accounts you did not open, and debts on your accounts that you can't explain. Check that information, like your Social Security number, addresses, name or initials, and employers is correct. Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

Call and speak with someone in the security or fraud department of each company. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures. If the identity thief has made charges or debits on your accounts, or has fraudulently opened accounts, ask the company for the forms to dispute those transactions.

File a complaint with the Federal Trade Commission. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces. You can file a complaint with the FTC using the Online Complaint Form.

https://rn.ftc.gov/pls/dod/widtpubls.startup?Z_ORG_CODE=PU03 or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338)

File a report with your local police or the police in the community where the identity theft took place. Then, get a copy of the police report or at the very least, the number of the report. It can help you work with creditors who need proof of the crime.

Again, please accept our sincerest apologies. Since this incident, we have taken steps to secure our physical security, data and equipment security and we are committed to fully protecting all of the information that is entrusted to us. If you have any questions, please contact Abigail Necesito at anecesit@advent.com.

Thank you for your patience and understanding.

Sincerely,

A handwritten signature in black ink, appearing to read "John Brennan". The signature is fluid and cursive, with a long horizontal line extending from the end.

John Brennan
Vice President, Human Resources

Advent Software, Inc.



Here are some answers to frequently asked questions:

1. When did the theft occur?

The week of November 20th

2. Were all previous employees affected?

No, only a subset of recent former employees was in the data.

3. What about dependents and partner information?

No, the data was only employee data.

4. What additional steps is Advent taking to make personal data more secure?

We are implementing additional security measures for laptops. We are in the process of deploying this, starting with the areas we have assessed to be of higher risk. We are also ensuring no personal employee data is downloaded or stored onto laptops.

5. Are dates of birth or bank account numbers involved?

No bank account numbers, direct deposit information, birthdates are involved.

6. Does asking a credit bureau to add a temporary 90 day fraud alert degrade an individual's credit standing, prevent issue of credit, or cause an increase in interest rates?

No. The 90 day fraud alert is an established industry standard precautionary procedure. Adding an optional voluntary extended alert in response to evidence of actual misuse of personal data can reduce the ability of businesses to fully use the credit file. For more information refer to <http://www.ftc.gov/bcp/edu/microsites/idtheft/> or <http://www.ssa.gov/pubs/idtheft.htm>